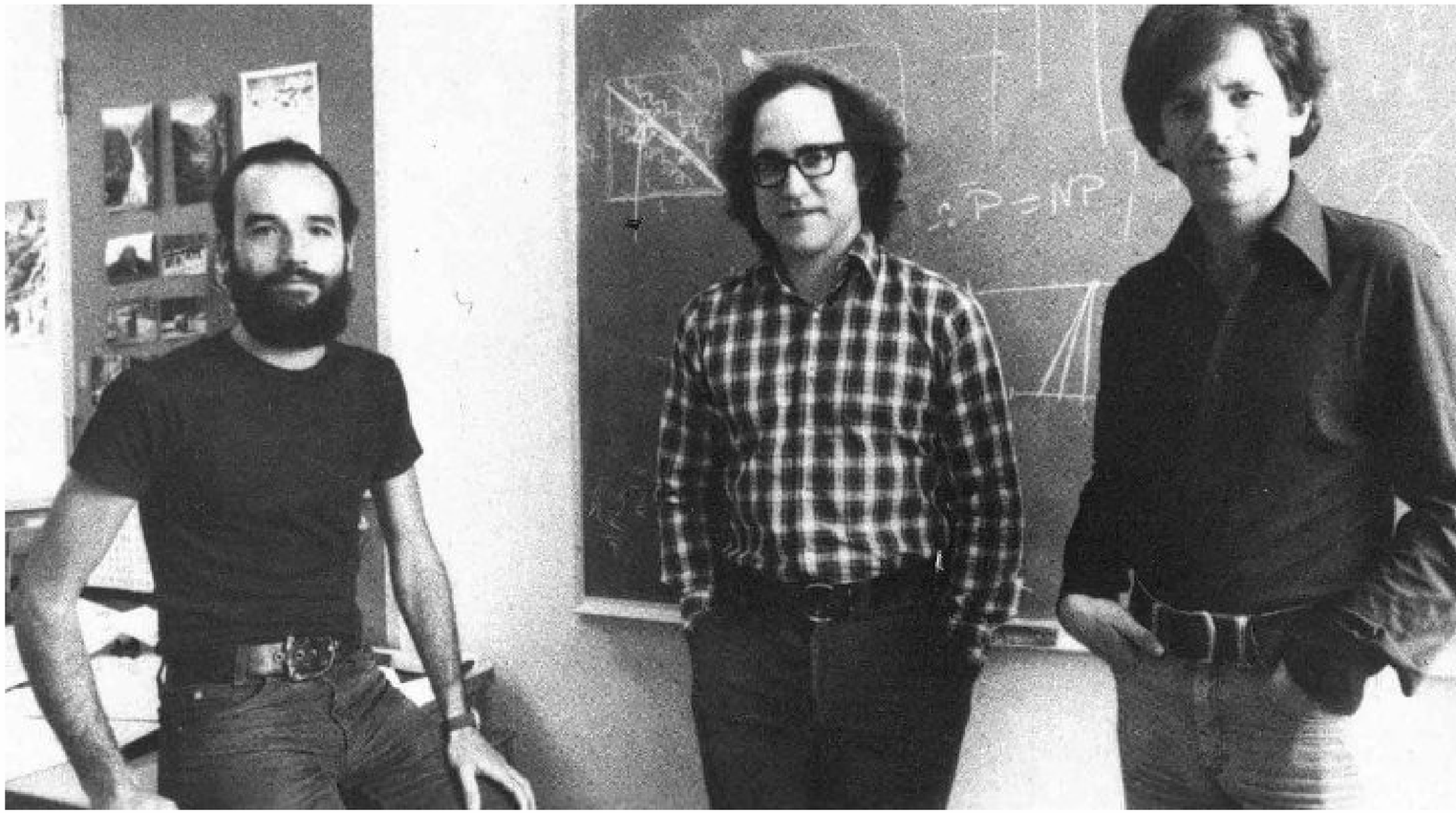
TRAVAIL PRATIQUE

MATHÉMATIQUES EN TECHNOLOGIE DE L'INFORMATION

h e p i a
Haute école du paysage, d'ingénierie et d'architecture de Genève

CHIFFREMENT

RIVEST SHAMIR ADLEMAN

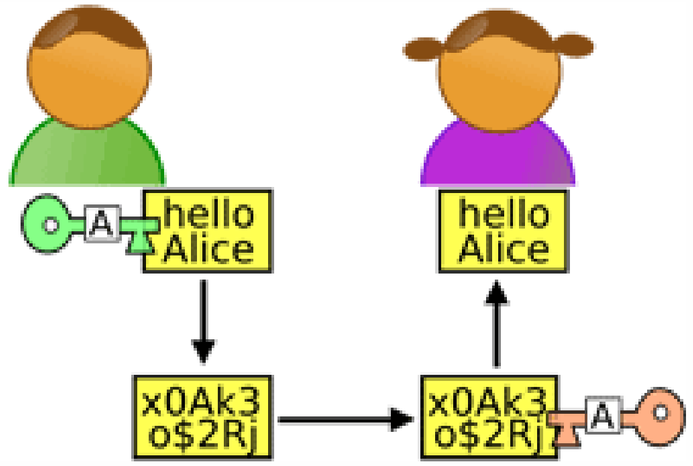


DYLAN MONTEIRO, KEVIN BONGA

Le travail pratique de chiffrement RSA est semblable à une mission de déchiffrement dans notre contexte

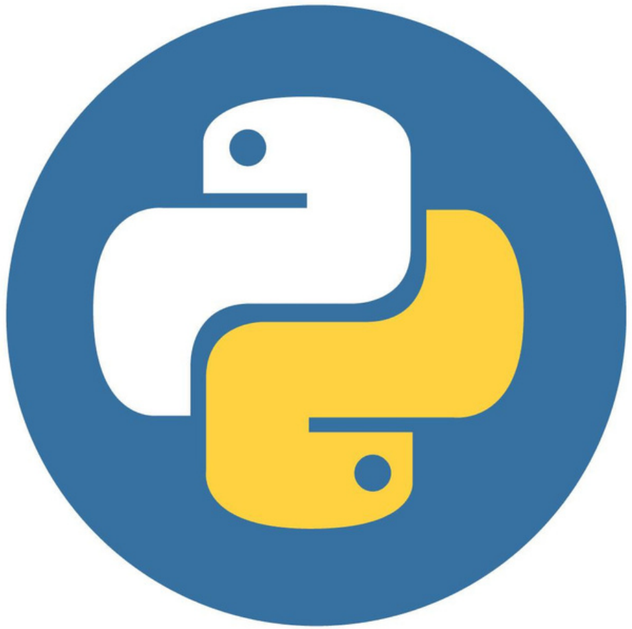
Agent Q du MI6 (James Bond - SKYFALL)

L'échange entre l'expéditeur et le destinataire de manière chiffrée s'effectue à l'aide de deux outils de base: la **clé publique** et la **clé privée**



Le RSA puise sa complexité de la factorisation en nombre premier

Le but du travail pratique est de déchiffrer un message chiffré



LOGO DU LANGAGE DE PROGRAMMATION PYTHON

A disposition :

- La clé publique
- L'exposant
- Le message codé sous forme de liste d'entier

Leonhard Euler
(Hopp Suisse)

- Trouver les nombres premiers facteurs (P&Q) de la clé publique fournie

- On calcule l'indicatrice d'Euler (Z) avec P & Q pour trouver l'inverse modulaire entre l'exposant et Z pour obtenir la clé privée (D)

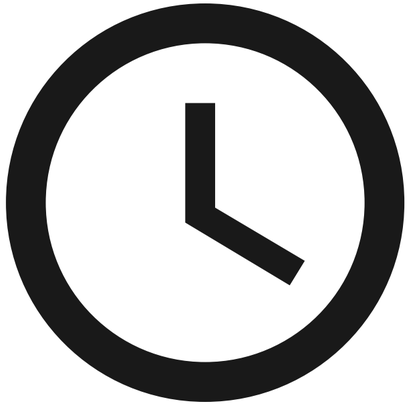
- Puis, nous utilisons l'exponentiation rapide sur chacun des entiers de la liste initiale à l'aide de la clé privée pour découvrir la valeur à décoder

- Nous convertissons la valeur obtenu en caractère au format UTF-8. Chaque valeur est ensuite ajouté à une string afin d'obtenir le message final.

Ah, mais c'est de là que ça vient ! Quand on dit "ça va comme sur des roulettes". En fait ça veut dire qu'le mec il peut balancer un morceau de rocher comme une catapulte, il continue quand même d'avancer d'façon mobile.

-Perceval (*Kaamelott*)

Pourquoi un résultat aussi rapide ?



En théorie, il faut des milliards d'années...

Merci pour votre attention